

Shuttlecock Association of Hong Kong, China

Guidelines and Procedures on Information Security

Issued in compliance with the Personal Data (Privacy) Ordinance (Cap. 486) Data Protection Principle 4, the PCPD Guidance Note on Data Security Measures for ICT, and the requirements of the Leisure and Cultural Services Department under the Sports Subvention Scheme

Document Ref.	Version	Effective Date	Approved by
SAHKC/IS/01	1.0	1 January 2027	Executive Committee

1. Purpose

These Guidelines set out the minimum measures that the Association and its staff must follow to protect the Association's information and information systems against unauthorised access, loss, alteration, leakage and disruption.

2. Scope

These Guidelines apply to all staff, Executive Committee members, coaches, team officials, volunteers and contractors who access the Association's information, computers, mobile devices, email accounts, websites, social media accounts or cloud services — whether Association-owned or personally owned.

3. Information Classification

Class	Examples	Handling rule
Confidential	Personal data, medical and anti-doping records, bank and payroll data, contracts, disciplinary files, passwords	Encrypt in storage and in transit; access strictly on a need-to-know basis approved by the Secretary General; never store on personal devices or public cloud accounts
Internal	Meeting papers, budgets, draft plans, internal correspondence	Share within the Association only; do not post publicly
Public	Published results, event notices, annual report	No restriction

4. Responsibilities

Role	Responsibility
Executive Committee	Approves these Guidelines; approves the annual IT budget; reviews security incidents and the annual security report.
Information Security Officer (ISO)	Appointed by the Executive Committee (in practice the Secretary General or his/her delegate). Maintains the asset and account inventory; grants and reviews access rights; manages backups, patching and vendors; leads

	incident response; arranges annual staff training.
All staff	Comply with these Guidelines; protect their accounts and devices; report incidents immediately.

5. Guidelines

5.1 Access Control and Accounts

- Every user has an individual account. Shared or generic accounts are not permitted, except for official social media accounts, for which the ISO keeps a controlled register of authorised users.
- Access is granted on a least-privilege, need-to-know basis and approved by the ISO.
- Passwords must be at least 12 characters and include a mix of letters, numbers and symbols; they must not be reused across services and must not be shared with anyone.
- Two-factor authentication must be enabled on email, cloud storage, banking, website administration and social media accounts.
- Accounts of departing staff must be disabled on the last working day. The ISO reviews all accounts and access rights at least annually.

5.2 Device and Workstation Security

- All computers and mobile devices used for Association work must have an up-to-date operating system, anti-malware software, a screen lock after 10 minutes of inactivity, and full-disk encryption where available.
- Security patches must be applied within one month of release; critical patches as soon as practicable.
- Devices must not be left unattended in public places. Clear-desk and clear-screen practice applies in the office.
- Personal devices may be used for Association work only with the ISO's approval, and must meet the same requirements. The Association may require remote wipe of Association data from a lost device.
- USB drives and portable media containing confidential information must be encrypted.

5.3 Email, Internet and Social Media

- Use Association email accounts for Association business; do not auto-forward Association email to personal accounts.
- Verify the recipient before sending. Use blind copy (Bcc) for group emails to members.
- Do not open unexpected attachments or links. Verify any payment or bank-account-change instruction by telephone with a known contact before acting on it.
- Do not post personal data, internal documents or images of minors on social media without consent and the approval of the Secretary General.

5.4 Data Storage, Transfer and Disposal

- Store Association records only on the Association's approved systems or approved cloud services; do not use personal cloud or messaging accounts to store Association records.
- Encrypt or password-protect confidential files before emailing or transporting them; send the password by a separate channel.
- Back up all critical data at least weekly, keep one copy off-site or in a separate cloud location, and test a restore at least once a year.

- Dispose of paper records by shredding and electronic media by secure wiping or physical destruction; keep a disposal record for confidential material.

5.5 Website and System Management

- The Association's website and online registration systems must use HTTPS and keep their software, plug-ins and components up to date.
- Administrator accounts must be limited in number, individually named and protected by two-factor authentication.
- A security risk assessment must be carried out before any new system or online service that handles personal data is launched, and periodically thereafter.

5.6 Third-Party and Vendor Management

- The ISO keeps a register of all IT vendors and cloud services used, including what data each holds.
- Contracts with vendors handling Association data must require adequate security measures, prohibit unauthorised use or sub-contracting, require immediate notification of any incident, and require return or deletion of data on termination.
- Vendor access to Association systems must be time-limited and revoked when the work is completed.

6. Procedures

6.1 Security Incident Response

- Step 1 — Report: staff must report any suspected incident (malware, phishing, lost device, unauthorised access, website defacement, suspicious payment request) to the ISO immediately and in any event within 24 hours. Do not attempt to fix it alone and do not delete evidence.
- Step 2 — Contain: the ISO isolates the affected device or account, resets credentials and stops any further loss.
- Step 3 — Assess: the ISO determines what information was affected. If personal data is involved, the Data Protection Officer is informed at once and the breach procedure in the Guidelines and Procedures on Personal Data Privacy Protection applies.
- Step 4 — Recover: restore from backup, apply fixes, and confirm normal operation.
- Step 5 — Report and learn: the ISO records the incident in the Incident Log, reports to the Executive Committee at its next meeting, and notifies the Police, the PCPD and LCSD where applicable.

6.2 Joiner, Mover and Leaver Procedure

- Joiner — the ISO creates accounts with approved access rights; the staff member signs the Acknowledgement at the Annex before access is granted.
- Mover — access rights are re-approved and unnecessary rights removed when a person changes role.
- Leaver — accounts are disabled on the last working day, devices and keys returned, and Association data removed from personal devices.

6.3 Backup and Business Continuity

- The ISO maintains a list of critical systems and data, with backup frequency and recovery responsibility.
- A restore test is performed at least annually and the result recorded.
- Key contact details and vendor support numbers are kept in an offline copy accessible in an emergency.

6.4 Training, Monitoring and Audit

- All staff receive an information security briefing on joining and a refresher at least once a year, covering phishing, password practice and incident reporting.
- The ISO performs an annual review covering accounts and access rights, patch status, backup tests, the vendor register and the incident log, and reports the results to the Executive Committee.
- The Association may, where resources permit, engage an independent party to review its information security.

7. Non-compliance

Failure to comply with these Guidelines may result in withdrawal of system access and disciplinary action. Unauthorised access to a computer or misuse of data may also give rise to criminal liability under the laws of Hong Kong.

8. Review

The ISO reviews these Guidelines at least every two years, or earlier following a significant security incident or a change in systems, the law or LCSD requirements. Revisions are approved by the Executive Committee.

9. References

- Personal Data (Privacy) Ordinance (Cap. 486), Data Protection Principle 4 — Security
- PCPD, "Guidance Note on Data Security Measures for Information and Communications Technology" (2022)
- Digital Policy Office / InfoSec.gov.hk — information security guidance for organisations
- Hong Kong Police Force CyberDefender — cyber security advice for non-profit organisations
- LCSD Sports Subvention Scheme — subvention agreement and corporate governance requirements

Enquiries: Information Security Officer, Shuttlecock Association of Hong Kong, China. Report incidents to the ISO immediately.

Annex — Staff Acknowledgement

I confirm that I have read and understood the Guidelines and Procedures on Information Security, and I agree to comply with it in the course of my duties with Shuttlecock Association of Hong Kong, China. I understand that non-compliance may lead to disciplinary action and, where the law is breached, to legal liability.

Name	Position	Signature	Date